

1 **In the Claims**

2 Claims 1, 8, 11, 18, 19, 25, 27, 28, 30 and 32 are currently amended.

3 Claims 1-33 are pending and are listed below.

4
5 1. (Currently Amended) A processor-readable medium having
6 a tangible component and comprising processor-executable instructions
7 configured for:

8 receiving a binary signature;

9 receiving a security patch;

10 identifying a vulnerable binary file on a computer based on the
11 binary signature; and

12 updating the vulnerable binary file on the computer with the
13 security patch.

14
15 2. (Original) A processor-readable medium as recited in claim
16 1, wherein the identifying a vulnerable binary file on a computer includes
17 comparing a bit pattern of the binary signature against binary files located
18 on the computer, the bit pattern associated with a security vulnerability.

19
20 3. (Original) A processor-readable medium as recited in claim
21 1, wherein the updating the vulnerable binary file on the computer includes
22 installing the security patch on the computer.

1 4. (Original) A processor-readable medium as recited in claim
2 1, wherein the identifying a vulnerable binary file on a computer includes
3 sending the binary signature to the computer.

4
5 5. (Original) A processor-readable medium as recited in claim
6 4, wherein the updating the vulnerable binary file on the computer
7 includes:

8 receiving a request from the computer to send the security patch;
9 and
10 sending the security patch to the computer.

11
12 6. (Original) A processor-readable medium as recited in claim
13 1, wherein the computer is a client computer and the receiving includes
14 receiving the binary signature and the security patch from a distribution
15 server configured to distribute to the client computer, binary signatures
16 that identify vulnerable files and security patches configured to fix the
17 vulnerable files.

18
19 7. (Original) A server comprising the processor-readable
20 medium as recited in claim 1.

21
22 8. (Currently Amended) A processor-readable medium having
23 a tangible component and comprising processor-executable instructions
24 configured for:
25

1 receiving a binary signature that identifies a security vulnerability
2 in a binary file;

3 receiving a security patch configured to fix the security
4 vulnerability in the binary file; and

5 distributing the binary signature and the security patch to a plurality
6 of servers.

7
8 9. (Original) A processor-readable medium as recited in claim
9 8, wherein the distributing includes:

10 sending a notice to each of the plurality of servers regarding the
11 security vulnerability and the available patch;

12 receiving a request to send the binary signature and the security
13 patch; and

14 sending the binary signature and the security patch in response to
15 the request.

16
17 10. (Original) A distribution server comprising the processor-
18 readable medium as recited in claim 8.

19
20 11. (Currently Amended) A processor-readable medium having
21 a tangible component and comprising processor-executable instructions
22 configured for:

23 receiving a binary signature from a server;

24 searching for the binary signature in binary files located on a client
25 computer;

1 sending a request from the client computer to the server for a
2 security patch if a binary file is found that includes the binary signature;
3 receiving the security patch from the server; and
4 updating on the client computer the binary file with the security
5 patch.

6
7 12. (Original) A client computer comprising the processor-
8 readable medium as recited in claim 11.

9
10 13. (Original) A method comprising:
11 receiving a binary signature;
12 searching for a vulnerable file based on the binary signature;
13 if a vulnerable file is found, requesting a security patch; and
14 fixing the vulnerable file with the security patch.

15
16 14. (Original) A method as recited in claim 13, wherein the
17 requesting includes sending a request to a server for the security patch, the
18 method further comprising receiving the security patch from the server in
19 response to the request.

20
21 15. (Original) A method as recited in claim 14, wherein the
22 receiving includes receiving the binary signature from the server.

23
24 16. (Original) A method as recited in claim 13, wherein the
25 fixing includes installing the security patch on a computer.

1 17. (Original) A method as recited in claim 13, wherein the
2 searching includes comparing the binary signature to binary information
3 on a storage medium of a computer.

4
5 18. (Currently Amended) A method as recited in claim 17,
6 wherein the binary information is selected from ~~the group~~ a group
7 comprising:

8 an operating system;
9 an application program file; and
10 a data file.

11
12 19. (Currently Amended) A method as recited in claim 17,
13 wherein the storage medium is selected from ~~the group~~ a group
14 comprising:

15 a hard disk;
16 a magnetic floppy disk;
17 an optical disk;
18 a flash memory card;
19 an electrically erasable programmable read-only memory; and
20 network-attached storage.

1 20. (Original) A method comprising:
2 receiving a binary signature and a security patch from a distribution
3 server;
4 searching on a client computer for a vulnerable file associated with
5 the binary signature; and
6 if a vulnerable file is found, fixing the vulnerable file with the
7 security patch.

8
9 21. (Original) A method as recited in claim 20, wherein the
10 searching includes transferring the binary signature to the client computer,
11 the client computer configured to search for a vulnerable file associated
12 with the binary signature.

13
14 22. (Original) A method as recited in claim 21, wherein the
15 fixing includes:
16 receiving a request from the client computer to transfer the security
17 patch, the client computer having located a vulnerable file; and
18 transferring the security patch to the client computer in response to
19 the request.

20
21 23. (Original) A computer comprising:
22 means for receiving a binary signature;
23 means for searching for a vulnerable file based on the binary
24 signature;
25

1 means for requesting a security patch if a vulnerable file is found;
2 and
3 means for fixing the vulnerable file with the security patch.
4

5 **24. (Original) A server comprising:**

6 means for receiving a binary signature and a security patch from a
7 distribution server;

8 means for scanning a client computer for a vulnerable file
9 associated with the binary signature; and

10 means for fixing the vulnerable file with the security patch if a
11 vulnerable file is found.
12

13 **25. (Currently Amended) A computer having a tangible**
14 **component and comprising:**

15 binary information;

16 a scan module configured to receive a binary signature and scan the
17 binary information for the binary signature; and

18 a patch module configured to request a security patch and install the
19 security patch if the binary signature is found in the binary information.
20

21 **26. (Original) A computer as recited in claim 25, further**
22 **comprising a storage medium configured to retain the binary information.**
23
24
25

1 27. (Currently Amended) A computer as recited in claim 25,
2 wherein the binary information is selected from ~~the group~~ a group
3 comprising:

4 an operating system;
5 an application program file; and
6 a data file.

7
8 28. (Currently Amended) A computer having a tangible
9 component and comprising:

10 binary files;
11 a binary signature; and
12 a security patch module configured to receive the binary signature
13 from a server and to scan the binary files in search of the binary signature.

14
15 29. (Original) A computer as recited in claim 28, further
16 comprising:

17 a binary file that includes the binary signature; and
18 a security patch;
19 wherein the security patch module is further configured to request
20 the security patch from the server upon locating the binary signature
21 within the binary file, and to apply the security patch to the binary file.

1 30. (Currently Amended) A distribution server having a tangible
2 component and comprising:

3 a database; and

4 a distribution module configured to receive a binary signature and a
5 security patch, store the binary signature and the security patch in the
6 database, and distribute the binary signature and the security patch to a
7 plurality of servers.

8
9 31. (Original) A distribution server as recited in claim 30,
10 wherein the distribution module is further configured to receive a request
11 from a server for the binary signature and the security patch and to
12 distribute the binary signature and the security patch to the server in
13 response to the request.

14
15 32. (Currently Amended) A server having a tangible component
16 and comprising:

17 a binary signature associated with a security vulnerability in a
18 binary file;

19 a security patch configured to fix the security vulnerability in the
20 binary file; and

21 a scan module configured to scan binary files on a client computer
22 for the binary signature and to update the binary file with the security
23 patch if the binary signature is found.

1 33. (Original) A server as recited in claim 32, further
2 comprising:

3 a database;

4 the scan module further configured to receive the binary signature and the
5 security patch from a distribution server and to store the binary signature and the
6 security patch in the database.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25